Secure quantum dense coding via tripartite entangled GHZ state in cavity QED

Zheng-Yuan Xue,* You-Min Yi, and Zhuo-Liang Cao†
Anhui Key Laboratory of Information Material & Devices,
School of Physics & Material Science, Anhui University, Hefei, 230039, P R China

We investigate economic protocol to securely encoding classical information among three users via entangled GHZ states. We implement the scheme in cavity QED with atomic qubits where the atoms interact simultaneously with a highly detuned cavity mode with the assistance of a classical field. The scheme is insensitive to the cavity decay and the thermal field, thus based on cavity QED techniques presently it might be realizable.

PACS numbers: 03.67.Hk, 03.65.Ud, 42.50.Dv

I. INTRODUCTION

Quantum entanglement, a fundamental feature of many-body quantum mechanical systems, was seen as a key resource for many tasks in quantum information processing. Among its novel applications, quantum dense coding (QDC) [1] and quantum secret sharing (QSS) [2] attract more and more public attention due to their promising application in secure direct quantum communication. QDC is a process to send two cbits of information, from a sender (Alice) to a remote receiver (Bob), by sending only a single qubit. It works in the following way. Initially, Alice and Bob shared a maximally entangled state. The first step is an encoding process where Alice performs one of the four local operations on her qubit, and then sends the qubit to Bob. The second step is a decoding process. After Bob received the qubit, he can discriminate the operation of Alice using only local operations (Bell state measurement in the pioneering work [1]). Recently, much attention has been paid to the studies of QDC both theoretically and experimentally.

In the realm of atom, cavity quantum electrodynamics (QED) techniques has been proven to be a promising candidate for the physical realization of quantum information processing. Recently, many schemes have been proposed for quantum entanglement engineering and quantum information processing [3]. The cavity usually act as memories in quantum information processing, thus the decoherence of the cavity field becomes one of the main obstacles for the implementation of quantum information in cavity QED. Recently, Zheng and Guo proposed a novel scheme [4], which greatly prolong the efficient decoherence time of the cavity. Osnaghi *et al.* [5] had experimentally implemented the scheme using two Rydberg atoms crossing a nonresonant cavity. Following the progress, schemes for implementing QDC in cavity QED are also proposed [6, 7].

QDC, despite for its novel classical capacity of sending classical information, should be very deliberately used for the sake of security of the process. If Bob is dishonest in the dense coding process, then he can always successfully cheat Alice and use the information willingly. Now, the question arises, is there any secure QDC scheme exist? Fortunately, We note that QSS is likely to play a important role in protecting secret quantum information. QSS is a process securely distribute private key among many parties. With the key, the sender, Alice can divide the message into two or more shares. If and only if when they cooperate, they can get complete information about the message. Meanwhile, if one of them is dishonest, the honest players may keep the dishonest one from doing any damage. Hence, after the pioneering work proposed by Hillery et al. [2], QSS attracts a great deal of attentions in both theoretical and experimental aspects.

In this paper, we investigate a secure QDC scheme with a tripartite GHZ state via QSS in cavity QED. The sender (Alice) can transmit two cbits of information by sending one qubit to one of the two receivers, *i.e.*, Bob. By collaboration, they could obtain the exact information of Alice, furthermore, any attempt to obtain the secret information without cooperation cannot be succeed in a deterministic way. Our scheme could work if one of them, and only one, is not entirely trustful.

II. QDC IN CAVITY QED

Suppose Alice wants to send secret information to a distant agent Bob, she possesses three qubits and they are in the GHZ state. As she does not know whether he is honest or not, she makes the information shared by two users (*i.e.*, Bob and Charlie). If and only if they collaborate, one of the users can read the information, furthermore, individual users could not do any damage to the process. Here, we base on the assumption that communication over a classical channel is insecure, which means we cannot result to the simplest method of teleportation [8] to distribute the information. Of course, one could also securely conquer the task using standard quantum cryptography, but, on average, it requires more resource and measurements [9]. Alice can generate a tripartite

*Electronic address: zyxue@ahu.edu.cn
†Electronic address: zlcao@ahu.edu.cn

entangled GHZ state [10] in cavity QED

$$|\psi\rangle_{1,2,3} = \frac{1}{\sqrt{2}}(|eee\rangle + i|gggg\rangle)_{1,2,3}, \quad (1)$$

where $|e\rangle$ and $|g\rangle$ are the excited and ground states of the atoms, respectively. Now, we present our scheme step by step.

Step 1. Alice decides to select one of the following two possible choices. With probability p, which is relatively very small, Alice selects the first choice of security checking, which aims to check the security of quantum channel, and the procedure continues to Step 2. Otherwise, Alice can decide to the information encoding step with probability $(1-p)$, the aim of which is to encode and implement the QDC procedure. In this case, the procedure goes to Step 3.

Step 2. Security checking. Hillery *et al.* [2] show that tripartite entangled GHZ state is sufficient to detect a potential eavesdropper in the channel.

Step 3. Information encoding. After Alice confirms that Bob and Charlie both receive their qubit from her, she performs one of the four local operations $(I, \sigma^x, i\sigma^y, \sigma^z)$ on her atom. These operations denote 2 cbits of information, and will transform state in Eq. (1) into

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|eee\rangle + i|ggg\rangle)_{1,2,3}, \quad (2a)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|gee\rangle + i|egg\rangle)_{1,2,3}, \quad (2b)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|gee\rangle - i|egg\rangle)_{1,2,3}, \quad (2c)$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|eee\rangle - i|ggg\rangle)_{1,2,3}. \quad (2d)$$

Now the information is encoded into the pure entangled state, which is shared among the three parties (Alice, Bob and Charlie), the encoding of the two cbits information is completed. Then Alice sends her atom to one of the two receivers (*i.e.*, Bob), we will latter prove that which is the party to send the atom to is not arbitrary. After a party receives the atom, he/she will get hold of two of all the three atoms, and thus he/she will have a higher probability of successful cheat compared with the one who have not in the QDC process. So, Alice would send her atom to the party, which is less likely to cheat.

Step 4. Information extracting. Assume Bob was selected to receive Alice's atom, and then he has two atoms. Next, We consider two identical two-level atoms simultaneously interacting with a single-mode cavity and simultaneously driven by a classical field. Then the interaction between the single-mode cavity and the two driven atoms can be described, in the rotating-wave approximation, as[11]

$$H = \omega_0 S_z + \omega_a a^+ a + \sum_{j=1}^{2}\{g(a^+ S_j^- + a S_j^+) + \Omega[(S_j^+ \exp(-i\omega t) + S_j^- \exp(i\omega t)]\} \quad (3)$$

where $S_z = 1/2\sum_{j=1}^{2}(|e\rangle_{j,j}\langle e| - |g\rangle_{j,j}\langle g|)$, $S_j^+ = |g\rangle_{j,j}\langle e|$, $S_j^- = |e\rangle_{j,j}\langle g|$ and $|e\rangle_j$, $|g\rangle_j$ are the excited and ground states of jth atom, respectively. a^+ and a are the creation and annihilation operators for the cavity mode, respectively. g is the coupling constant between cavity and particle, Ω is the Rabi frequency, ω_0 , ω_a and ω are atomic transition frequency, cavity frequency and the frequency of the driven classical field, respectively.

While the case of $\omega_0 = \omega$, the evolution operator of the system, in the interaction picture, is $U(t) = \exp(-iH_0 t)\exp(-iH_e t)$, where $H_0 = \sum_{j=1}^{2}\Omega(S_j^+ + S_j^-)$, H_e is the effective Hamiltonian. In the strong driving regime $\Omega \gg \delta, g$ (δ been the detuning between atomic transition frequency ω_0 and cavity frequency ω_a) and the case of $\delta \gg g$, there is no energy exchange between the atomic system and the cavity thus the scheme is insensitive to both the cavity decay and the thermal field. Then in the interaction picture, the effective interaction Hamiltonian reads[11]

$$H_e = \frac{\lambda}{2}[\sum_{j=1}^{2}(|e\rangle_{j,j}\langle e| + |g\rangle_{j,j}\langle g|) + \sum_{j=1;i\neq j}^{2}(S_j^+ S_k^+ + S_j^+ S_k^- + H.c.)] \quad (4)$$

where $\lambda = g^2/2\delta$. If two atoms are simultaneously sent into the cavity and simultaneously interact with it. Using the above cavity, it is easy to verify the following evolvement

$$|g\rangle|g\rangle \rightarrow e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle)(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle) - i\sin\lambda t(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle)(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle)]. \quad (5a)$$

$$|g\rangle|e\rangle \rightarrow e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle)(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle) - i\sin\lambda t(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle)(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle)]. \quad (5b)$$

$$|e\rangle|g\rangle \rightarrow e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle)(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle) \\ -i\sin\lambda t(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle)(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle)]. \quad (5c)$$

$$|e\rangle|e\rangle \rightarrow e^{-i\lambda t}[\cos\lambda t(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle)(\cos\Omega t|e\rangle - i\sin\Omega t|g\rangle) \\ -i\sin\lambda t(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle)(\cos\Omega t|g\rangle - i\sin\Omega t|e\rangle)]. \quad (5d)$$

Choosing to adjust the interaction time $\lambda t = \pi/4$ and modulate the driving field $\Omega t = \pi$, lead the quantum state of the three atoms system in Eq. (2), after interaction, to

$$|\psi_1\rangle = \frac{1}{2}[|ee\rangle_{1,2}(|e\rangle + |g\rangle)_3 - i|gg\rangle_{1,2}(|e\rangle - |g\rangle)_3], \quad (6a)$$

$$|\psi_2\rangle = \frac{1}{2}[|ge\rangle_{1,2}(|e\rangle + |g\rangle)_3 - i|eg\rangle_{1,2}(|e\rangle - |g\rangle)_3], \quad (6b)$$

$$|\psi_3\rangle = \frac{1}{2}[-i|eg\rangle_{1,2}(|e\rangle + |g\rangle)_3 + |ge\rangle_{1,2}(|e\rangle - |g\rangle)_3], \quad (6c)$$

$$|\psi_4\rangle = \frac{1}{2}[-i|gg\rangle_{1,2}(|e\rangle + |g\rangle)_3 + |ee\rangle_{1,2}(|e\rangle - |g\rangle)_3]. \quad (6d)$$

Obviously, one can see that there is an explicit correspondence between Alice's operation and the measurements results of the two receivers, which means that if they cooperate, both of them can get the information. But if they do not choose to cooperate, neither of the two users could obtain the information by local operation in a deterministic manner. In this way, we complete the procedure of secret extraction, and the above procedures from step 1 to step 4 constitute a complete process of secure QDC.

step 5. Repeat the above steps until all the secret information have been transmitted.

III. DISCUSSION

Now, we turn to the case if they do not choose to cooperate with each other. Without the cooperation of Charlie, Bob still knows which type Alice's operation belongs to, (I, σ^z) or $(\sigma^y, i\sigma^y)$. But he cannot further discriminate which one Alice's operation is. Without the cooperation of Bob, Charlie knows nothing about Alice's operation. If Charlie lies to Bob, Bob also has a probability of 1/2 to get the correct information, so the successful cheat probability of Charlie is 1/2. Conversely, Charlie only has a probability of 1/4 to get the correct information, so the successful probability of Bob is 3/4. This is the point that we addressed above, he who received Alice's atom has a higher probability of successful cheat compared with the party who have not. If there is an eavesdropper, he may be one of Bob and Charlie, or another one besides the three parties. The eavesdropper has been able to entangle an ancilla with the GHZ state, and at some later time she can measure the ancilla to gain information about the measurement results of the users. However, Hillery *et al.* [2] show that if this entanglement does not introduce any errors into the procedure, then the state of the system is a product of the GHZ triplet and the ancilla, which means the eavesdropper could gain nothing about the measurements on the triplet from observing his/her ancilla.

We also note the scheme can generalize to multi-users case providing Alice possesses a multipartite entangled state. Suppose she has a $(N+1)$-qubit entangled state, qubits $2, 3, \cdots (N+1)$ are to N users, respectively. After she confirms that each of the users have received a qubit, she then operates one of the four local measurements on qubit 1. After that, the two cbits information was encoded into the $(N+1)$-qubit entangled state. Later, she sends her qubit to one of the rest N users. Again, he who received the qubit will have a higher probability of successful cheat compared with the rest (N-1) users. Only with the cooperation of all the rest users, one can obtain Alice's information. In this way, we set up a secure network for QDC via QSS.

Next, we will give a brief analysis of the experimental feasibility of our scheme. During the process, our scheme only involves atom-field interaction with a large-detuned cavity and does not require the transfer of quantum information between the atoms and cavity. In addition, with the help of a strong classical driving field the photon-number dependent parts in the evolution operator are canceled. Thus the scheme is insensitive to both the thermal field and the cavity decay. So, the requirement on the quality factor of the cavities is greatly loosened. Meanwhile it is noted that the atomic state evolution is independent of the cavity field state, thus based on cavity QED techniques presently [4, 5] it might be realizable. In our scheme, the two atoms must be simultaneously interaction with the cavity. But in real case, we can't achieve simultaneousness in perfect precise. Calculation on the error suggests that it only slightly affects the fidelity of the reconstruct state [4].

IV. SUMMARY

In summary, we have investigated a secure scheme for QDC with GHZ type entangled state Via QSS in cavity QED. If and only if when they cooperate with each

other, they can read the original information. Any attempt to get complete information of the state without the cooperation of the third party cannot be succeed in a deterministic way. In the scheme we provide a way to achieve all operations of dense coding, from generation of the entangled state to various measurements, by using cavity QED techniques. we The distinct advantage of the scheme is that during the passage of the atoms through the cavity field, a strong classical field is accompanied, thus the scheme is insensitive to both the cavity decay and the thermal field. Furthermore, our scheme only employs single-qubit computational basis measurements, thus it may offer a simple and easy way of demonstrating secure QDC experimentally in cavity QED via QSS.

Acknowledgments

This work is supported by Anhui Provincial Natural Science Foundation under Grant No: 03042401, the Key Program of the Education Department of Anhui Province under Grant No: 2002kj029zd and 2004kj005zd and the Talent Foundation of Anhui University.

[1] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[2] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, (1999) 1829.
[3] J. M. Raimond, M. Brune and S. Haroche, Rev. Mod. Phys. **73** 565 (2001).
[4] S. B. Zheng and G. C. Guo, Phys. Rev. Lett. **85**, 2392 (2000).
[5] S. Osnaghi, P. Bertet, A. Auffeves, P. Maioli, M. Brune, J. M. Raimond, and S. Haroche, Phys. Rev. Lett. **87**, 037902 (2001).
[6] X. M. Lin, Z.W. Zhou, P. Xue, Y. J. Gu and G. C. Guo, Phys. Lett. A **313**, 351 (2003).
[7] L. Ye and G. C. Guo, Phys. Rev. A **71**, 034304 (2005).
[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[9] C.H. Bennett, G. Brassard, and N. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[10] G. P. Guo, C. F. Li, J. Li and G. C. Guo, Phys. Rev. A. **65**, 042102 (2002).
[11] S. B. Zheng, Phys. Rev. A **68**, (2003) 035801.